君合专题研究报告 JUNHE

2021 年 6 月 29 日

软件产品如何才算“安全”？——从供应商角度看软件安全要求

随着近年来信息技术的飞速发展，以及社会对“万物互联”时代的期盼，软件产品在实践应用中也正面临着前所未有的风险和挑战。根据《国家网络空间安全战略》[1]，重视软件安全，加快安全可信产品推广应用，是夯实网络安全基础的重要环节。《外商投资安全审查办法》更是将投资“重要信息技术和互联网产品与服务”并取得所投资企业的控制权的情形明确纳入外商投资安全审查的范围。软件安全的重要性日益凸显。

一般而言，软件包括系统性软件、支持性软件、应用性软件等，而软件的构成涉及编程、数据与文档资料的收集等方面。软件安全是一种系统级的问题，不仅需要考虑安全的措施、机制（比如访问控制），还需要考虑基于安全的设计（比如用于防范木马病毒或恶意攻击的设计）。考虑到软件安全也属于计算机安全与网络安全的一部分，而网络与信息安全被明确列入国家安全范畴。目前我国法律法规对软件安全的要求覆盖软件产品从设计、生产到实际投入运营或使用的全过程，安全保障义务涉及软件产品的供应商、采购者和运营者等多个主体。保障软件产品在投入使用前的合规性，对软件安全整体而言不可或缺。因此，本文拟主要从供应商的角度，简要介绍软件产品合规相关的法律法规与各类标准。

一、软件产品安全涉及的法律标准

2009年，工信部曾发布《软件产品管理办法》（已失效）对软件产品进行登记备案管理。随着该管理办法被废止，我国不再以单独部门规章的形式对软件产品的开发、生产、销售、进出口等活动进行管理，而是将软件产品并入网络产品与信息产品中，适用产品质量责任、进出口贸易、网络安全审查等多个领域的安全合规要求。

1、产品质量责任

根据《中华人民共和国产品质量法》（以下简称“**《产品质量法》**”），“产品”须具备两个条件：一是经过加工、制作，未经过加工制作的自然物不是产品；二是用于销售，应当是可以进入流通领域的物。软件是特殊类型的智力产品，对于智力产品是否属于《产品质量法》所规范的“产品”，我国立法并未明确规定。但是我们注意到司法实践及监管部门执法中，存在将《产品质量法》规定明确适用于软件产品的情况，要求相关软件产品的生产者与销售者依照《产品质量法》的规定承担产品质量责任[2]。

具体而言，《产品质量法》中涉及产品安全的要求主要包括两方面：一是不存在危及人身、财产安全的不合理的危险；二是有保障人体健康和人身、财产安全的国家标准、行业标准的，应当符合该标准。在不符合《产品质量法》要求的情况下，软件的生产者或将承担民事、行政乃至刑事责任。

2、进出口贸易

[1]国家互联网信息办公室 2016 年 12 月 27 日发布：http://www.xinhuanet.com/politics/2016-12/27/c_1120196479.htm

[2]在北京普度信息技术有限公司上诉赛贝斯软件（中国）有限公司等产品责任纠纷【(2016)京 01 民终 4516 号】一案中，一审法院与二审法院均适用《产品质量法》就涉案软件的质量问题作出裁定。

在全球化背景下，软件进出口活动日益频繁。软件进出口贸易的形式可以分为通过光盘、磁盘等进行的有介质进出口，以及通过网络传输的无介质进出口。其中，软件的无介质进出口涉及数字服务贸易，无需履行海关的进出口检验检疫程序，而软件的有介质进出口属于实体进出口，涉及海关的进出口商品检验。

根据《中华人民共和国进出口商品检验法》规定的进出口商品检验目的，保障进出口软件安全属于进出口商品检验的题中之义。《中华人民共和国进出口商品检验法实施条例》进一步将进出口商品区分为法定检验产品（包括列入目录的进出口商品，以及法律、行政法规规定须经检验的其他进出口商品）与抽查检验产品。法定检验产品与抽查检验产品应当按照国家技术规范的强制性要求、国家商检部门指定的国外有关标准或者海关总署指定的其它相关技术要求进行检验。若所进出口的软件未达到相关标准或技术要求，可能在海关检验时遭遇阻碍，无法进出口；规避海关要求擅自进出口，则可能面临没收违法所得、罚款乃至刑事责任的处罚。

3、网络安全审查

作为网络产品的一种，软件产品同样需适用于致力于推广安全可信的网络产品和服务的《中华人民共和国网络安全法》（以下简称“**《网络安全法》**”）。该法将网络产品和服务的合规要求分为三类，未能达到要求的主体可能面临行政处罚。

第一类要求适用于所有网络产品和服务的提供者，主要见于《网络安全法》第22条，包括符合相关国家标准的强制要求、不得设置恶意程序、发现存在安全缺陷及漏洞等风险时及时采取补救措施、提供安全维护、符合个人信息保护规定等方面。

第二类要求适用于网络关键设备和网络安全专用产品的提供者。根据《网络安全法》第23条的规定，除了符合相关国家标准的强制要求外，若要提供或销售此类软件产品，还应当由具备资格的机构安全认证合格或者安全检测符合要求。

第三类要求虽然适用于关键信息基础设施的运营者，但由于安全审查的对象包括所采购的产品和服务，因此相关软件产品的供应商需确保其提供的软件产品符合安全审查的要求。此类审查中重点评估的因素具体可见于《网络安全审查办法》第9条，包括关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损等多个方面。

4、软件行业协会的双软评估

如前所述，工信部曾发布《软件产品管理办法》对软件企业、软件产品（包括国产软件与进口软件）进行登记备案，通常称为“双软认证”。在《软件产品管理办法》废除前，双软认证为强制要求。在该管理办法废除后，软件供应商为体现产品合规，也可能自愿在各地软件行业协会进行软件企业和软件产品的评估，即“双软评估”。

目前，双软评估所适用的标准为《软件产品评估标准》（T/ SIA 003—2019）和《软件企业评估标准》（T/ SIA 002—2019）。[3]其中，对软件产品的合规要求可分为两个层面：一是就软件产品的内容做出规定，包括不得侵犯他人知识产权、不得含有计算机病毒、不得危害计算机系统安全、不得含有禁止传播的内容、符合我国软件标准规范等；二是在提交评估时，要求供应商提供由软件检测机构出具的检测证明或类似材料。

二、软件产品安全涉及的行业标准

从上文可以看出，虽然软件产品安全的要求涉及多个领域的法律法规，但法律法规对安全的要求较为概括化，实践中仍应参考相关行业标准的具体要求。因此，我们也针对部分情境下软件安全可能涉及的具体标准进行了梳理。

虽然目前关于软件的标准均为推荐性质，但部分适用于信息安全产品类软件的推荐性标准根据有关部门的规范性文件实质上具有了强制效力（详见下文分析），具有较高的参考价值。此外，我们观察到许多国际最佳安全标准已被领先软件产品

[3] https://srpg.csia.org.cn/#/site/policyShow/policyList

供应商应用以保障软件产品安全，例如《信息安全管理实施细则》（ISO/IEC 17799-1）、《信息安全管理标准》（ISO/IEC 27001）、《信息技术 安全技术 漏洞的披露》（ISO/IEC 29147）等，为国内软件产品安全提供了良好实践参考。

1、一般软件产品

适用于一般软件产品的既有安全标准主要包括《信息安全技术 网络产品和服务安全通用要求》[4]（GB/T 39276-2020）、《信息安全技术 应用软件安全编程指南》[5]（GB/T 38674-2020）、《信息安全技术 信息技术产品安全可控评价指标》系列国家标准[6]（GB/T 36630-2018）、《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则》（GB/T 25000.51-2016）、《信息技术 安全技术 信息技术安全评估准则》（GB/T 18336-2015）等推荐性国家标准，这些标准不仅对软件提出“独立可靠”、“安全可控”等通用要求，还就软件的开发、生命周期支持、测试与评价等多个环节提供了技术操作上的指导。

2、信息安全产品类软件

根据《中华人民共和国认证认可条例》，“列入目录的产品，必须经国务院认证认可监督管理部门指定的认证机构进行认证。”对于所规定的相关产品，未经认证，不得出厂、销售、进口或者在其他经营活动中使用。因此，被列入《第一批信息安全产品强制性认证目录》[7]的信息安全产品类软件，除满足一般软件产品的通用安全要求外，还需参照所对应的国家标准进行强制性认证。例如，被要求进行强制性认证的防火墙软件产品必须根据《信息安全技术 防火墙安全技术要求和测试评价方法》[8]（GB/T 20281-2020）进行认证，反垃圾邮件产品则需要根据《信息安全技术反垃圾邮件产品技术要求和测试评价方法》[9]（GB/T 30282-2013）进行认证。虽然所依据的国家标准仅为推荐性质，但根据强制性认证的相关文件，[10]上述国家标准实质上被赋予了强制效力。

3、特殊场景类软件产品

在某些特殊场景下使用的软件产品还可能适用特殊的标准。例如，针对在移动智能终端使用的应用软件与操作系统，《信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法》[11]（GB/T 34975-2017）与《信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法》[12]（GB/T 34976-2017）即对软件产品的安全技术与安全保障进一步提出了与安装、卸载等方面相关的要求。

同时，不同行业尤其是敏感领域也可能适用其他特殊标准。以金融行业中所使用的证券期货业软件为例，中国证监会已发布《证券期货业软件测试规范》（JR/T 0175-2019）、[13]《证券期货业软件测试指南 软件安全测试》（JR/T 0191-2020）、[14]《证券期货业移动互联网应用程序安全规范》（JR/T 0192-2020）[15]等金融行业推荐性标准，供各经营机构参考以加强对移动终端应用的安全管理。类似的，航空行业涉及广泛复杂的生产组合，且与公众安全密切相关，工业和信息化部针对航空业的软件开发规定了《民用飞机机载系统和设备软件合格审定保证指南》（HB/Z 421-2014）作为专业技术参考。

[4] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=671EE0F00774EC5E980A9DC0E803751A
[5] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=910B7DBAEB214FE027F163E361960208
[6] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=A5D652978E2045FF92199E77276FE6B4
[7] 参见《国家质量监督检验检疫总局、国家认证认可监督管理委员会公告 2008 年第 7 号——关于部分信息安全产品实施强制性认证的公告》。
[8] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=DC339A62C32B0B5C64F567DD5F09EDE0
[9] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=DD9A9FF3DEACD42D14C492F65AA25DE8
[10] 《国家认证认可监督管理委员会公告 2014 年第 6 号—关于变更国家信息安全产品认证部分认证依据标准的公告》、《国家认监委公告 2016 年第 15 号——关于部分产品依据新版标准实施国家信息安全产品认证的公告》中明确规定了对具体信息安全产品进行强制性认证所应当适用的国家标准。
[11] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=D00C1CE888B129CF3F00B6618AF2897E
[12] http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=D95EF3840CECE4264BE55093F12D3729
[13] http://www.csrc.gov.cn/pub/zjhpublic/zjh/201910/P020191018544638414121.pdf
[14] http://www.csrc.gov.cn/pub/zjhpublic/zjh/202007/P020200717621887461887.pdf
[15] http://www.csrc.gov.cn/pub/zjhpublic/zjh/202007/P020200717621887627667.pdf

三、总结

综合来看，我国软件安全所涉及的领域较多。由于相关的法律法规仅对软件安全提出了原则性要求，实践中很大程度上需参考相关标准。现行的软件安全标准均为推荐性质，仅有部分标准通过相关文件在实践中被赋予强制效力，整体上缺乏影响力和约束力。随着互联网及软件的不断发展，有理由相信软件安全规范也将相应得到发展。

值得注意的是，今年6月刚通过的《中华人民共和国数据安全法》创设了数据分级分类保护、数据安全风险管控制度、数据安全审查制度等数据领域的基本制度。前述制度的具体配套法规、管理制度，以及其与相关现有法规的衔接有待进一步观察。软件产品作为数据的重要载体，待数据领域的基本制度进一步明确后可能需要相应调整产品的安全性，以符合数据安全的制度要求。

君合将持续保持关注并进一步梳理相关要求，以供对相关话题感兴趣的人士参考。

张静宇　合伙人　电话：86 10 8553 7718　邮箱地址：zhangjy@junhe.com
陆雯婷　律　师　电话：86 10 8519 1257　邮箱地址：luwt@junhe.com
刘　薇　实习生